

TITLE OF THE INVENTION

PROGRAM WRITABLE IC CARD AND METHOD THEREOF

BACKGROUND OF THE INVENTION

Field of the Invention

5 The present invention relates to an IC card having a writable memory and more particularly to an IC card for writing a program in this memory by keeping security and a method thereof.

Description of the Prior Art

10 An IC card is excellent in security and finds wide applications. Generally, an IC card has a built-in memory for writing and storing a program as well as various information which can be erased electrically and is used to write various information after a user
15 owns it. For example, the invention disclosed in Japanese Laid-Open Patent Application 6-309558 stores customer information in an IC card and provides quick services. In Japanese Laid-Open Patent Application 6-309384, a use that inspection results and dosing data
20 of a patient in a medical institution are stored in an IC card is described. Furthermore, recently, study has been given to use of an IC card in an electronic money system and an IC card is used to write money information.

25 As mentioned above, the use method of writing

information in an IC card is generally carried out. To keep security, the use method of changing and adding to an internal program stored already and writing a new program is limited.

5 To improve or change the function of an IC card, there is a case that changing of a program is necessary. Furthermore, to keep security, a case that changing of the cryption method is necessary also may be caused. However, to make it possible to modify an
10 already stored program leads to information opening to public of the microprocessor chip of the IC card and the program thereof and it is not suitable for the use of this IC card for which high security is evaluated.

SUMMARY OF THE INVENTION

15 Therefore, an object of the present invention is to provide an IC card for changing or adding to an internal program with the high security of an IC card kept and writing a new program and a method thereof.

To accomplish this object, the present invention
20 is a program writable IC card comprising a microprocessor and a memory for storing a program write control program having at least one of the decryption function and the function for converting a program code and a program for the aforementioned
25 microprocessor, wherein when the program for the

microprocessor is given from the outside, the IC card performs at least one of the decryption process and the process of converting a program code according to the program write control program and stores the program in the memory.

More concretely, according to the present invention which is a program writable IC card comprising a microprocessor and a memory storing a program for the microprocessor, one characteristic is a constitution that the IC card includes a write control program having the decryption function and/or the program code conversion function in a program built in the IC card and a memory for program writing and the other characteristic is a constitution that the IC card includes a write control microprocessor for executing the write control program having the decryption function and/or the program code conversion function in addition to the microprocessor for IC card, a means for switching the two microprocessors, and a memory for program writing.

Another characteristic of the present invention is a constitution that the IC card having a microprocessor whose technical information such as a specification is not opened to public includes a microprocessor whose technical information such as a

catalog and a specification is opened to public, a memory for program writing for storing a program for the microprocessor, and a means for switching the two microprocessors.

5 These constitutions make it possible to change or add to an internal program by keeping the security necessary for the IC card and to write a new program.

10 The foregoing and other objects, advantages, manner of operation and novel features of the present invention will be understood from the following detailed description when read in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

15 Fig. 1 is a block diagram showing a first embodiment of the program writable IC card of the present invention.

 Fig. 2 is a block diagram showing a second embodiment of the program writable IC card of the present invention.

20 Fig. 3 is a block diagram showing a third embodiment of the program writable IC card of the present invention.

 Fig. 4 is a block diagram showing a fourth embodiment of the program writable IC card of the present invention.

25

Fig. 5 is a block diagram showing a fifth embodiment of the program writable IC card of the present invention.

Fig. 6 is a block diagram showing a sixth embodiment of the program writable IC card of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 is a block diagram showing a first embodiment of the writable IC card of the present invention. Numeral 1 indicates a microprocessor for IC card, 2 a connector with an external device, 3 a program ROM (1), 3A a program for realizing the IC card function, 3B a write control program having decryption function, 4 a memory for writing, and L1 a data bus.

The microprocessor for IC card 1, the connector 2, and the IC card function program 3A are components for realizing the original function of the IC card. An external instruction is given to the microprocessor 1 via the connector 2 and the IC card performs an operation according to this instruction. A write command for instructing writing is incorporated in the IC card function program 3A beforehand and the IC card function program 3A activates the write control program 3B by an external write instruction. The write

control program 3B is provided with the decryption function beforehand and when the write control program 3B is activated, communication with the IC card requires a crypted command and data, a cryption key, and others. If a program, command, and data to be written later are not crypted correctly, they are rejected by the write control program 3B and the program and data cannot be written into the memory for writing 4. If a program to be written later is crypted, even if it is opened to public, a problem of loss of security will not arise and there is no need to manage the program writing process strictly. Therefore, in addition to keeping of security for a program in the IC card, security can be kept also for a program to be written later.

Fig. 2 is a block diagram showing a second embodiment of the writable IC card of the present invention. Numeral 1 indicates a microprocessor for IC card, 2 a connector with an external device, 3 a program ROM (1), 3A a program for realizing the IC card function, 3C a write control program having program code conversion function, 4 a memory for writing, and L1 a data bus.

The microprocessor for IC card 1, the connector 2, and the IC card function program 3A are components for

realizing the original function of the IC card and the operations thereof are the same as those of the aforementioned first embodiment. A write command for instructing writing is incorporated in the IC card function program 3A beforehand and the IC card function program 3A activates the write control program 3C by an external write instruction. This write control program 3C has a function for converting a program code and a program to be written later is processed by this write control program 3C, converted in a different format from that of a code inputted from the connector 2, and then written into the memory for writing 4. This program to be written later is created in a location where the security thereof is managed and the program code thereof is converted beforehand according to a rule which is reverse to the program code conversion rule in the write control program 3C. By doing this, in the same way as with the first embodiment, in addition to keeping of security for a program in the IC card, security can be kept also for a program to be written later.

If the function of a prior art for converting a program code for microprocessor to a program code for microprocessor in an IC card which is not open to public is provided as a program code conversion

function of the write control program 3C, there is no need to open the information on the microprocessor 1 in the IC card to public for a program developer.

Namely, from an advantage that a program code to be given from the outside may be a known code and there is no need to open an instruction code of a program in the IC card to the outside, the security of the IC card can be kept and furthermore the program development efficiency can be improved. In this case, from a viewpoint of keeping of security, adding of a function for eliminating fetching of information on the IC card function program 3A by a program to be written later is effective.

If the write control program 3C has both the two functions explained in the first and second embodiments, that is, the decryption function and the program code conversion function, it is more effective in the respect of security keeping of the IC card.

Fig. 3 is a block diagram showing a third embodiment of the writable IC card of the present invention. Numeral 1 indicates a microprocessor for IC card, 2 a connector with an external device, 3 a program ROM (1), 3A a program for realizing the IC card function, 4 a memory for writing, 5 a microprocessor for writing, 6 a program ROM (2), 6A a

write control program having decryption function, 7 a switch, L1 a data bus, L2 a switching signal (1), and L3 a switching signal (2). The switch 7 is a means for selectively switching the microprocessors 1 and 5

5 connected to the connector 2 and switches them by the switching signals L2 and L3. When the switch 7 selects the microprocessor 1, the microprocessor 1, the connector 2, and the program ROM (1) 3 realize the original IC card function.

10 A write command for instructing writing is incorporated in the IC card function program 3A beforehand, and the switching signal (1) L2 is outputted from the IC card for microprocessor 1 by a write instruction from the outside, and the switch 7
15 is switched to the microprocessor for writing 5. The write control program 6A is provided with the decryption function. The write control program 6A executes the decryption function by the microprocessor for writing 5. Communication with the IC card after
20 the switch 7 is switched to the microprocessor for writing 5 requires a crypted program, command, and data, a cryption key, and others. If a program, command, and data to be written later are not crypted correctly, they are rejected by the write control
25 program 6A and the program and data cannot be written

into the memory for writing 4. Therefore, in addition to keeping of security for a program in the IC card, security can be kept also for a program to be written later. When the IC card is structured like this, even
5 if it can be switched to the write mode by an incorrect operation, if the process ends normally and the switch 7 cannot be returned to the microprocessor for IC card 1 by the switching signal L3, the use as an ordinary IC card can be made impossible forever and
10 the security can be kept. This is an advantage which is not found in the first and second embodiments. Even in a constitution that one microprocessor is used, if it is used incorrectly, by adding a circuit receiving no external reset signal, the same effect can be
15 obtained. Since the two microprocessors 1 and 5 are independent of each other, a microprocessor in a quite different format can be used and a constitution with higher security can be obtained.

Fig. 4 is a block diagram showing a fourth
20 embodiment of the writable IC card of the present invention. Numeral 1 indicates a microprocessor for IC card, 2 a connector with an external device, 3 a program ROM (1), 3A a program for realizing the IC card function, 4 a memory for writing, 5 a
25 microprocessor for writing, 6 a program ROM (2), 6B a

write control program having program code conversion function, 7 a switch, L1 a data bus, L2 a switching signal (1), and L3 a switching signal (2). The functional operation of this embodiment as an IC card and the switching operation for the two microprocessors are the same as those of the third embodiment mentioned above. This embodiment has both the functions of the second and third embodiments mentioned above.

If the write control program 6B is provided with both of the two functions explained in the third and fourth embodiments, that is, the decryption function and the program code conversion function, it is more effective in the respect of keeping of security of the IC card.

Fig. 5 is a block diagram showing a fifth embodiment of the writable IC card of the present invention. This embodiment shows a program writable IC card for keeping the internal security of the IC card by perfectly opening a program to be written later to the user side. Numeral 1 indicates a microprocessor for IC card, 2 a connector with an external device, 3 a program ROM (1), 3A a program for realizing the IC card function, 3D a program for write control, 4 a memory for writing, 7 a switch, 8 a microprocessor

whose information is opened to public, L1 a data bus,
L2 a switching signal (1), L3 a switching signal (2),
and L4 a chip select signal. A program to be written
into the memory for writing 4 is structured so as to
5 be executed only by the microprocessor whose
information is opened to public 8. The chip select
signal L4 for the program ROM (1) 3 storing the IC
card function program 3A is structured so as to be
controlled only by the microprocessor for IC card 1.
10 Therefore, it is impossible to access the program ROM
(1) 3 by a program to be written later and the
security of the IC card function can be kept.

The program writing operation for the memory for
writing 4 is started when the microprocessor for IC
15 card 1 activates the program for write control 3D by
an external write instruction. The program for write
control 3D performs a process of writing an external
program and data into the memory for writing 4. The
program in this case is created for the microprocessor
20 whose information is already opened to public 8 and
the security of the IC card function is kept inside
the IC card, so that there is no need to protect a
program to be written later.

This embodiment is a one which is suited to a use
25 for making openly handling a program to be written

later and keeping the security as an IC card compatible with each other.

Fig. 6 is a block diagram showing a sixth embodiment of the writable IC card of the present invention. Numeral 1 indicates a microprocessor for IC card, 2 a connector with an external device, 3 a program ROM (1), 3A a program for realizing the IC card function, 4 a memory for writing, 7 a switch, 8 a microprocessor whose information is opened to public, 6 a program ROM (2), 6C a write control program for the microprocessor 8, L1 a data bus, L2 a switching signal (1), L3 a switching signal (2), and L4 a chip select signal. The respect of keeping the security of the IC card function by the chip select signal L4 is the same as that of the fifth embodiment.

According to this embodiment, the program ROM (2) 6 storing the write control program 6C for the microprocessor whose information is opened to public 8 is independent of the program ROM (1) 3 storing the IC card function program 3A, so that keeping of the security of the IC card function can be enhanced more.

When a program is to be written later, the microprocessor for IC card 1 passes the control process to the microprocessor whose information is opened to public 8 by the switching signal L2. The

microprocessor whose information is opened to public 8
performs all the write control process according to
the write control program 6C and returns the control
process to the microprocessor for IC card 1 by the
5 switching signal L3 when the write process ends.

According to the fifth and sixth embodiments, the
development efficiency can be improved by use of a
microprocessor whose information is opened to public
under a catalog specification or operation
10 specification. However, by combining the function for
controlling writing like the other embodiments, the
security for a program to be written later can be kept.

The memory for writing program 4 has no
independent constitution and can serve as a memory for
15 program of a microprocessor if it is writable.

In each aforementioned embodiment, a memory which
can write only once can be used for the aforementioned
memory for writing.

Effects of the Invention

20 As mentioned above, according to the present
invention, an IC card which keeps the security of the
IC card function high and can write a program later
can be obtained.